



PATENT ABSTRACTS OF JAPAN

(↑↑) Publication number: 2000122539 A

(43) ~~Date of publication of application:~~ 28 . 04 . 00

(51) Int. Cl. G09C 1/00
G06F 12/14
G01B 20/10
H04L 9/10

(21) Application number: 16295837

(22) Date of filing: 16 . 10 . .98

(71) Applicant: MATSUSHITA ELECTRIC IND CO
LTD

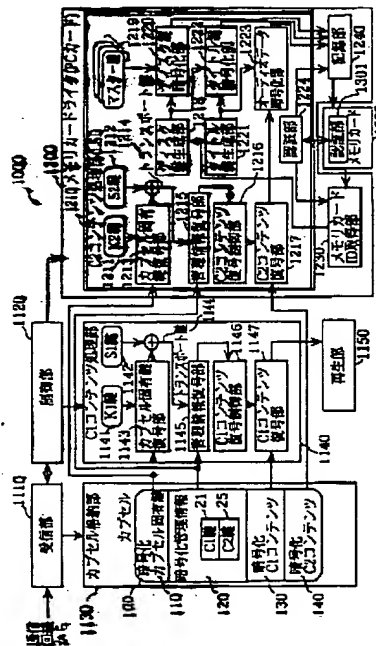
(72) Inventor: MATSUZAKI NATSUME
HARADA TOSHIHARU

(54) BOOK PROTECTION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a book protection system; preventing deciphered contents from being illegally peeped into during a recording process after ciphered contents are deciphered once and as ciphered.

SOLUTION: A personal computer receives a capsule 100 containing ciphered C2 contents 140 from a communication line, and the C2 contents are deciphered by a C2 contents deciphering part 1217 in a C2 contents processing part 1210 which is a tamper-resistant LSI package in a memory card writer 1200 of a PC card, and an audio data ciphering part 1223 ciphers the entire or a part of the deciphered C2 contents and outputs it to a recording part 1245. The recording part 1240 records the data ciphered in the C2 contents processing part 1210 on a memory card 1300 which is a semiconductor memory inserted into a memory card writer 1200.



COPYRIGHT: (C)2000, JPO

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-122539

(P2000-122539A)

(43)公開日 平成12年4月28日(2000.4.28)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 5 B 0 1 7
	6 2 0		6 2 0 Z 5 D 0 4 4
	6 4 0		6 4 0 B 5 J 1 0 4
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
G 1 1 B 20/10		G 1 1 B 20/10	H

審査請求 未請求 請求項の数14 O L (全 15 頁) 最終頁に続く

(21)出願番号 特願平10-295837

(22)出願日 平成10年10月16日(1998.10.16)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 原田 俊治

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 100090446

弁理士 中島 司朗 (外1名)

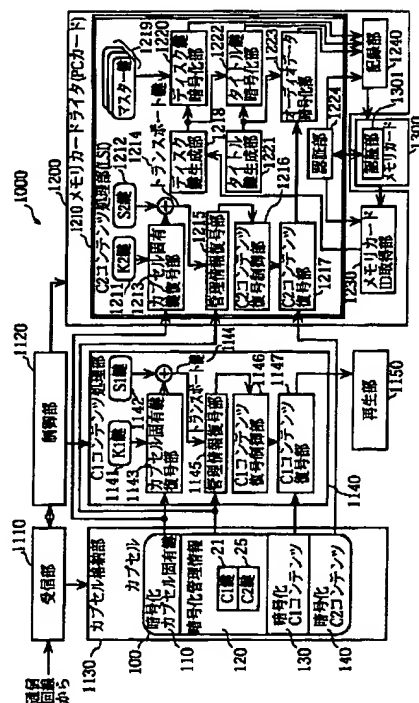
最終頁に続く

(54)【発明の名称】 著作物保護システム

(57)【要約】

【課題】 暗号化されたコンテンツを一度復号して再度暗号化して記録媒体に記録する過程において、復号されたコンテンツが不正に覗き見されないような著作物保護システムを提供する。

【解決手段】 パーソナルコンピュータにより、暗号化C2コンテンツ140を含むカプセル100を通信回線から受信し、C2コンテンツを、PCカードであるメモリカードライタ1200中の耐タンパ性のあるLSIパッケージであるC2コンテンツ処理部1210内でC210コンテンツ復号部1217により復号し、その復号したC2コンテンツの全部又は一部をオーディオデータ暗号化部1223が暗号化して記録部1240に出力する。記録部1240は、メモリカードライタ1200に挿入された半導体メモリであるメモリカード1300に、C2コンテンツ処理部1210内で暗号化されたデータを記録する。



1

【特許請求の範囲】

【請求項1】 外部から入力されたデジタル著作物である暗号化されたコンテンツを復号し、再暗号化して出力する著作物保護システムであって、

入力されたコンテンツを第1の暗号方式で復号する復号手段と、

前記復号手段により復号されたコンテンツの全部又は一部を第2の暗号方式で暗号化して出力する暗号化手段とを備え、

前記復号手段、前記暗号化手段、及び前記復号手段から10
前記暗号化手段へのデータの通信路が単一の耐タンパ性のあるパッケージに封入され、

外部との入出力のための端子が前記パッケージの外部に表出しており、

前記復号手段は、前記端子を通じて入力を受け付け、前記暗号化手段は、前記端子を通じて出力することを特徴とする著作物保護システム。

【請求項2】 前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータ通信路は、1
チップの半導体集積回路から構成されていることを特徴とする請求項1記載の著作物保護システム。

【請求項3】 前記復号手段あるいは前記暗号化手段は、鍵データを記憶しており、復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムを、前記端子を通じて外部ネットワークよりダウンロードし、前記コンテンツを前記鍵データを用いて前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記鍵データを用いて前記暗号アルゴリズムにより暗号化することを特徴とする請求項1又は2記載の著作物保護システム。

【請求項4】 前記復号手段はさらに、前記端子を通じてコンテンツの復号に関する暗号化された制御情報を取得すると共に取得した制御情報を復号する制御情報復号部と、

前記復号部により復号された制御情報に基づいて前記コンテンツの復号を行うコンテンツ復号部とを有することを特徴とする請求項1～3記載のいずれか1項に記載の著作物保護システム。

【請求項5】 前記暗号化手段は、
マスター鍵を記憶するマスター鍵記憶部と、
ディスク鍵を生成するディスク鍵生成部と、
前記マスター鍵を用いて、前記ディスク鍵生成部により生成された前記ディスク鍵を暗号化するディスク鍵暗号化部と、
タイトル鍵を生成するタイトル鍵生成部と、
前記ディスク鍵を用いて、前記タイトル鍵生成部により生成された前記タイトル鍵を暗号化するタイトル鍵暗号化部と、
前記タイトル鍵を用いて、前記復号手段により復号されたコンテンツの一部又は全部のデータを暗号化するデー

2

タ暗号化部と、

前記ディスク鍵暗号化部により暗号化されたディスク鍵と、前記タイトル鍵暗号化部により暗号化されたタイトル鍵と、前記データ暗号化部により暗号化されたデータとを前記端子を通じて出力する出力部とを有することを特徴とする請求項1～4のいずれか1項に記載の著作物保護システム。

【請求項6】 前記マスター鍵記憶部は、複数のマスター鍵を記憶し、

前記ディスク鍵暗号化部は、複数の前記マスター鍵それぞれを用いて、前記ディスク鍵を暗号化することにより、複数の暗号化されたディスク鍵を生成することを特徴とする請求項5記載の著作物保護システム。

【請求項7】 前記暗号化手段はさらに、前記マスター鍵を外部ネットワークよりダウンロードして前記マスター鍵記憶部に追加する、あるいは、特定マスター鍵を無効化するマスター鍵制御部を有することを特徴とする請求項5又は6記載の著作物保護システム。

【請求項8】 前記暗号化手段により暗号化の結果として得るデータは、記録媒体に記録されるべきものであり、

前記記録媒体には、予め媒体に固有な固有情報が記録されており、

前記ディスク鍵生成部は、前記記録媒体中の前記固有情報に基づいて前記ディスク鍵を生成することを特徴とする請求項5～7のいずれか1項に記載の著作物保護システム。

【請求項9】 前記タイトル鍵生成部は、前記復号手段により復号されたコンテンツの一部の情報、又は前記暗号化手段に固有な情報に基づき、前記タイトル鍵を生成することを特徴とする請求項5～8のいずれか1項に記載の著作物保護システム。

【請求項10】 前記記録媒体は、記録装置認証部を備え、

前記出力部は、前記記録媒体の前記記録装置認証部から受信する認証情報に基づいて前記記録媒体の正当性を判定し、正当である場合にのみ、前記出力を行うことを特徴とする請求項5～9のいずれか1項に記載の著作物保護システム。

【請求項11】 前記復号手段は、前記コンテンツの復号に際し、当該復号に対する課金処理を行うことを特徴とする請求項1～10記載の著作物保護システム。

【請求項12】 前記復号手段あるいは前記暗号化手段は、外部ネットワークよりダウンロードした復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムについて署名情報を確認して、正当であった場合にのみ、以後、前記コンテンツを前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記暗号アルゴリズムにより暗号化することを特徴とする請求項3記載の著作物保護システム。

3

【請求項13】 前記マスター鍵制御部は、外部ネットワークよりダウンロードした前記マスター鍵について署名情報を確認して、正当であった場合にのみ、前記マスター鍵を前記マスター鍵記憶部に格納する、あるいは、無効化制御について、署名情報を確認して、正当であった場合にのみ、前記特定マスター鍵の無効化を行うことを特徴とする請求項7記載の著作物保護システム。

【請求項14】 前記パッケージは、記録媒体に前記コンテンツを記録する記録装置に内蔵され、前記暗号化手段は、前記記録媒体に前記コンテンツの全10部又は一部を記録するための所定の規格化された暗号化方式に従った暗号化を行うものであり、前記復号手段に入力される前記コンテンツに施されている暗号化は、前記コンテンツの配送元と、前記記録装置との間における特有の暗号化方式により、前記コンテンツを安全に配送するためになされたものであることを特徴とする請求項1又は2記載の著作物保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ディジタル著作物20の著作権保護技術に関し、特に、ネットワークを介して配送されるコンテンツを記録媒体に記録する場合に用いる著作権保護技術に関する。

【0002】

【従来の技術】 近年、インターネット関連技術の発展により、音楽等のコンテンツをインターネットを通じて配送し、これをダウンロードしたユーザから料金等を受け取ることも可能となってきた。また、インターネットからパーソナルコンピュータにダウンロードされたディジタル著作物が簡単に複製できるものであるため、これを30防止するために、暗号化技術を用いてコンテンツを暗号化して配送することも可能である。

【0003】

【発明が解決しようとする課題】 ネットワークを介して配送する有償のコンテンツが不正にコピー等されることを回避するために、コンテンツの提供者は、インターネット等を通じてコンテンツを暗号化して配送し、購入者は、配送されたコンテンツを専用の記録媒体に記録した後、その記録媒体を専用の再生装置に挿入して再生させることができるというようなコンテンツの流通形態が考40えられる。この場合、コンテンツの内容は専用の記録媒体においても暗号化されるべきであるが、専用の記録媒体を小型化することその他の目的により専用の記録媒体においては、ネットワーク上で配送されるための暗号化とは異なる暗号化、例えばより小規模のアルゴリズムで実現できる暗号化を施す必要がある場合もある。また、記録媒体への記録のための暗号化について、各メーカーの協議により規格化されている場合もある。なお、この場合、この規格に従って記録された記録媒体は、各メーカーの再生装置で再生可能となる。

4

【0004】 しかしながら、ネットワーク上で配送されるために暗号化されたコンテンツを、一度復号してから再度記録媒体に記録するための暗号化を施すと、復号から再暗号化までの経路において、復号されたコンテンツが不正に覗き見される危険が生じる。そこで、本発明は、このような問題点に鑑みてなされたものであって、暗号化されたコンテンツを一度復号して再度暗号化して記録媒体に記録する過程において、復号されたコンテンツが不正に覗き見されないような著作物保護システムを提供することを目的とする。

【0005】

【課題を解決するための手段】 上記課題を解決するために、本発明に係る著作物保護システムは、例えばネットワークを介して、外部から入力されたディジタル著作物である暗号化されたコンテンツを復号し、記録用に再暗号化して出力する著作物保護システムであって、入力されたコンテンツを第1の暗号方式で復号する復号手段と、前記復号手段により復号されたコンテンツの全部又は一部を第2の暗号方式で暗号化して出力する暗号化手段とを備え、前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータの通信路が単一の耐タンパ性のあるパッケージに封入され、外部との入出力のための端子が前記パッケージの外部に表出しており、前記復号手段は、前記端子を通じて入力を受け付け、前記暗号化手段は、前記端子を通じて出力することを特徴とする。

【0006】 上記構成により、暗号化されたコンテンツを一度復号して再度暗号化する過程において、復号されたコンテンツが不正に覗き見されないようになる。

【0007】

【発明の実施の形態】 以下、本発明に係る著作物保護システムの実施の形態である音楽コンテンツ再生記録システムについて、図面を用いて説明する。

<構成> 図1は、本発明の実施の形態に係る音楽コンテンツ再生記録システム1000の外観図である。

【0008】 音楽コンテンツ再生記録システム1000は、通信回線1001を介して受信した音楽コンテンツをパーソナルコンピュータ1100により再生し、また、メモ리카ード1300に記録するシステムである。なお、メモ리카ード1300は、厚さ数ミリ、縦横2cm四方程度の形状で、64メガバイトの記憶容量をもち制御回路を内蔵する半導体メモリである。ユーザは、このメモ리카ード1300を、メモ리카ード再生機器に挿入することにより、ヘッドフォン等を通じて再生された音楽を楽しむことができる。

【0009】 同図に示すように、音楽コンテンツ再生記録システム1000は、ディスプレイ1191とキーボード1192とを備えるパーソナルコンピュータ1100と、これに挿入されるメモ리카ードライタ1200とから構成される。パーソナルコンピュータ1100は、

5

CPU、メモリ、ハードディスク等を内蔵し、ユーザに指示に応じて音楽コンテンツ再生用のプログラムを実行することができるものであり、スピーカ1193及び通信回線1001と接続されており、また、いわゆるPCカードスロットであるメモリカードライタ挿入口1195を有する。

【0010】メモリカードライタ1200は、いわゆるPCカードであり、メモリカードを挿入するためのメモリカード挿入口1299を有している。図2は、音楽コンテンツ再生記録システム1000の機能ブロック図である。機能的には、音楽コンテンツ再生記録システム1000は、受信部1110と、制御部1120と、カプセル格納部1130と、C1コンテンツ処理部1140と、再生部1150と、メモリカードライタ1200とから構成される。同図には、音楽コンテンツ再生記録システム1000自体の他、メモリカードライタ1200に挿入されるメモリカード1300と、通信回線から受信部1110が受信してカプセル格納部1130に格納するカプセル100とをも示している。ここで、カプセル100は、通信回線から音楽コンテンツ再生記録システム1000に入力されるデータであり、音楽コンテンツとこれに関する管理情報等が暗号化されたものである。カプセル100の内容については後に詳しく説明する。

【0011】受信部1110と、制御部1120と、C1コンテンツ処理部1140と、再生部1150とはパーソナルコンピュータ1100のメモリに格納された音楽コンテンツ再生用のプログラムがCPUにより実行されることによって実現される機能であり、カプセル格納部1130は、パーソナルコンピュータ1100のメモリ又はハードディスクの一領域である。

【0012】音楽コンテンツ再生用のプログラムは、受信すべき音楽コンテンツをユーザに選択させたり、選択された音楽コンテンツを再生するか、記録するか等のユーザの指示を受け付けるためのものであり、制御部1120は、キーボード1192によるユーザ操作を受け付け、これに応じて、音楽コンテンツの受信指示、再生指示、記録指示等を行うものである。

【0013】受信部1110は、制御部1120からの受信指示を受けて、インターネットに接続された通信回線1001から暗号化された音楽コンテンツを含むデータであるカプセルを受信して、カプセル格納部1130に格納し、カプセルの格納場所を制御部1120に通知する。カプセルは音楽コンテンツの供給会社等からインターネット等を通じて配送される。ここでは説明のため、図2に示すように、受信部1110によりカプセル格納部1130にはカプセル100が格納されたものとする。

【0014】C1コンテンツ処理部1140は、制御部1120から、再生指示とカプセル100の格納場所に50

6

ついでの情報とを受けると、カプセル100中の暗号化C1コンテンツ130を復号するための処理を行い、復号したC1コンテンツを再生部1150に出力する。音楽コンテンツには、16KHzのサンプリングレートでサンプリングされた低音質の試聴用のものと、64KHzのサンプリングレートでサンプリングされた高音質の購入用のものと2種類のものが存在し、ここでは、前者をC1コンテンツといい、後者をC2コンテンツという。暗号化C1コンテンツ130は、C1コンテンツを暗号化したものであり、暗号化C2コンテンツ140は、C2コンテンツを暗号化したものである。なお、C1コンテンツ処理部1140の詳細については、カプセル100の内容と共に後に詳細に説明する。

【0015】再生部1150は、C1コンテンツ処理部1140から渡されたC1コンテンツを再生してスピーカ1193を鳴らす機能部分であり、音楽コンテンツはMPEG (Moving Picture Experts Group) オーディオの規格に則って圧縮されているものであるため、再生部1150はこれを伸張する機能をも有する。

【0016】メモリカードライタ1200は、図3に示すようなハードウェア構造を有するPCカードであり、制御部1120から記録指示とカプセル100の格納場所についての情報とを受け取ると、カプセル100中の暗号化C2コンテンツ140を復号して再度別の暗号化を施してメモリカード1300に記録する機能を有するものである。

【0017】図3は、メモリカードライタ1200のハードウェア構造を示す図である。同図に示すように、メモリカードライタ1200は、ハードウェア的には、CPU1201と、ROM1202と、RAM1203と、PCインタフェース1204と、メモリカードインタフェース1205と、複数の端子をもつLSIであるC2コンテンツ処理部1210とがバス接続されたものであり、PCインタフェース1204を介してPCMCIA (Personal Computer Memory Card International Association) 規格に従いパーソナルコンピュータ1100とデータの通信を行い、メモリカードインタフェース1205を介してメモリカード1300とデータの通信を行う。

【0018】ここで、CPU1201は、ROM1202に記録されたプログラムを実行しメモリカードライタ1200の制御を行うものであり、RAM1203を作業用の領域として用いる。また、C2コンテンツ処理部1210は、電流供給用の導線で巻き付けられ全面的に包まれた耐タンパ性を有するLSIパッケージである。耐タンパとは、外部からの不正なアクセスに対して防御可能なことである。C2コンテンツ処理部1210は、1つのシリコン基盤上に形成された、即ち、1チップの

集積回路である。また、C2コンテンツ処理部1210は、電氣的、物理的に内部データを検査することが不可能となっており、例えば、LSIパッケージの内部データがEEPROMに保持されており、LSIパッケージを開けようとする導線が切断されることになり、これによりLSIパッケージへの電流の供給が停止し、コンデンサに貯えられた電荷からなる内部データがクリアされるような構造となっている。

【0019】メモ리카ードライタ1200は、機能的には、図2に示すように、C2コンテンツを復号し、オーディオデータ記録用のための暗号化を施すC2コンテンツ処理部1210と、メモ리카ード1300から個々のメモ리카ードに固有なメモ리카ードIDを取得するメモ리카ードID取得部1230と、暗号化されたオーディオデータをメモ리카ード1300に記録する記録部1240とを備える。なお、C2コンテンツ処理部1210は、メモ리카ード1300の正当性を認証するための認証部1224をも含む。C2コンテンツ処理部1210の処理内容の詳細については後述する。

<データ構造と関連処理>以下、カプセル100の内容20について説明する。カプセル100は、著作権保護センタにより生成されるデータである。ここで著作権保護センタとは、著作権保護のための中立的な機関をいう。著作権保護センタは、上述した音楽コンテンツの供給会社等から音楽コンテンツとこれに関連する管理情報等を受け取り、これらを暗号化してカプセル100を生成する。

【0020】音楽コンテンツ再生記録システム1000に入力されるカプセル100は、図1に示すように、160ビットの暗号化カプセル固有鍵110と、固定長の30暗号化管理情報120と、内容に応じてデータ長が変わり得る暗号化C1コンテンツ130と、内容に応じてデータ長が変わり得る暗号化C2コンテンツ140とから構成されるデータである。

【0021】図4は、暗号化C1コンテンツ130及び暗号化C2コンテンツ140の生成過程を示すデータフロー図である。同図に示すように、暗号化C1コンテンツ130は、平文であるC1コンテンツ30をC1鍵21で暗号化することにより生成されるデータである。C1鍵21は64ビットの鍵データであり、暗号化はブロック暗号方式で行い、例えばDES(Data Encryption Standard)アルゴリズムが用いられる。

【0022】また、暗号化C2コンテンツ140は、平文であるC2コンテンツ40をC2鍵25で暗号化することにより生成されるデータである。C2鍵25は128ビットの鍵データであり、暗号化は、ブロック暗号方式で行い、例えばDESアルゴリズムに準じたアルゴリズムが用いられる。なお、C1コンテンツ30及びC2コンテンツ40はそれぞれ、MPEGオーディオの規格50

に基づき圧縮されている。

【0023】図5は、暗号化カプセル固有鍵110及び暗号化管理情報120の生成過程を示すデータフロー図である。同図に示すように、暗号化管理情報120は、管理情報20をトランスポート鍵1144で暗号化することにより生成されるデータである。ここで、管理情報20は、図4に示したC1コンテンツ30及びC2コンテンツ40に関連した情報であり、C1鍵21、C1アドレス22、C1復号条件情報23、C1課金情報24、C2鍵25、C2アドレス26、C2復号条件情報27、C2課金情報28を含む。また、暗号化3における暗号化アルゴリズムはブロック暗号方式のものであり、例えばDESアルゴリズムに準じたアルゴリズムが用いられる。

【0024】ここで、C1アドレス22及びC2アドレス26は、それぞれカプセル100内における暗号化C1コンテンツ130の相対アドレス、暗号化C2コンテンツ140の相対アドレスを示す。C1復号条件情報23及びC2復号条件情報27は、それぞれC1コンテンツ30、C2コンテンツ40を復号するための条件を示す情報であり、復号することを許容する期日等を示すものである。また、C1課金情報24及びC2課金情報28は、それぞれC1コンテンツ30、C2コンテンツ40を復号する際に請求されるべき料金に関する情報、即ち、音楽コンテンツの試験料金や購入料金を示す情報である。

【0025】トランスポート鍵1144は、著作権保護センタが任意に定める160ビットの鍵データである。また、図5に示すように、暗号化カプセル固有鍵110は、トランスポート鍵1144とS1鍵1142との排他的論理和により得られるカプセル固有鍵10を、楕円秘密鍵5で、楕円暗号方式のアルゴリズムにより暗号化して生成されるデータである。ここで、S1鍵1142は、音楽コンテンツ再生記録システム1000のC1コンテンツ処理部1140に記憶されているS1鍵と同値の160ビットの共通鍵である。また、楕円秘密鍵5は、C1コンテンツ処理部1140に記憶されている公開鍵であるK1鍵1141と対となる160ビットの秘密鍵である。なお、楕円暗号については、Douglas R. Stinson著「暗号理論の基礎」(共立出版株式会社)に詳細に説明されている。

【0026】以下、上述のように生成されたカプセル100の内容に関連した処理を行うC1コンテンツ処理部1140及びC2コンテンツ処理部1210の処理内容について詳細に説明する。まず、C1コンテンツ処理部1140の処理内容について説明する。C1コンテンツ処理部1140は、K1鍵1141及びS1鍵1142を記憶しており、また、カプセル固有鍵復号部1143と、管理情報復号部1145と、C1コンテンツ復号制御部1146と、C1コンテンツ復号部1147とを構

成要素とする。

【0027】カプセル固有鍵復号部1143は、カプセル100内の暗号化カプセル固有鍵110を、公開鍵であるK1鍵1141を用いて復号化して出力する。出力されたカプセル固有鍵と、共通鍵であるS1鍵1142との排他的論理和の結果であるトランスポート鍵1144を用いて、管理情報復号部1145は、カプセル100内の暗号化管理情報120を復号する。

【0028】C1コンテンツ復号制御部1146は、復号された管理情報20中のC1復号条件情報23を参照10することにより復号可否を判断して、復号可能な場合には、C1課金情報24を参照して課金処理を行い、C1コンテンツ復号部1147に復号指示を与える。ここで、課金処理とは、通信回線を介して、ユーザが予め契約している銀行等の口座から、音楽コンテンツの供給会社等に、試聴料金を送金するような旨の指示情報を送信することである。なお、試聴は無料である場合には、前記指示情報の送信は行わない。

【0029】C1コンテンツ復号部1147は、管理情報復号部1145により復号された管理情報20中のC201アドレス22を参照して暗号化C1コンテンツ130の位置を特定し、管理情報20中のC1鍵21を用いて、暗号化C1コンテンツ130を復号し、再生部1150にC1コンテンツ30を出力する。なお、復号アルゴリズムは、図4に示す暗号化1に対応するブロック暗号方式のアルゴリズムである。

【0030】次に、C2コンテンツ処理部1210の処理内容について説明する。C2コンテンツ処理部1210の処理内容は、C2コンテンツの復号と、メモ리카ードへの記録のための再暗号化とに大別されるが、C2コ30ンテンツの復号に関しては、上述のC1コンテンツ処理部1140の処理と類似している。C2コンテンツ処理部1210は、C2コンテンツの復号機能を行うために、K2鍵1211及びS2鍵1212を記憶し、カプセル固有鍵復号部1213と、管理情報復号部1215と、C2コンテンツ復号制御部1216と、C2コンテンツ復号部1217とを構成要素としており、さらに、メモ리카ードへの記録のための再暗号化機能を行うために、複数のマスター鍵1219を記憶し、ディスク鍵生成部1218と、ディスク鍵暗号化部1220と、タイ40トル鍵生成部1221と、タイトル鍵暗号化部1222と、オーディオデータ暗号化部1223と、認証部1224とを構成要素としている。ここで、マスター鍵とは、各メーカーのメモ리카ード再生装置に保持されている鍵データと同値の鍵データであり、その内容は、各メーカー毎に異なる。記録すべきメモ리카ードが複数のメーカーのメモ리카ード再生装置で再生できるように、C2コンテンツ処理部1210には、複数のメーカーについてのマスター鍵1219が記憶されている。

【0031】カプセル固有鍵復号部1213は、カプセル

ル100内の暗号化カプセル固有鍵110を、公開鍵であるK2鍵1211を用いて復号化して出力する。出力されたカプセル固有鍵と、S2鍵1212との排他的論理和の結果であるトランスポート鍵1214を用いて、管理情報復号部1215は、カプセル100内の暗号化管理情報120を復号する。ここで、トランスポート鍵1214は、上述したC1コンテンツ処理部1140において得られたトランスポート鍵1144と同値である。なお、K2鍵1211とS2鍵1212とは、図5における楕円秘密鍵5を、公開鍵であるK2鍵1211に対応する楕円秘密鍵に置き換えるとともに、図5におけるS1鍵1142をS2鍵に置き換えても、図5に示すようにトランスポート鍵1144に基づいて暗号化カプセル固有鍵110が生成できるような関係にある鍵データである。

【0032】C2コンテンツ復号制御部1216は、管理情報復号部1215により復号された管理情報20中のC2復号条件情報27を参照することにより復号可否を判断して、復号可能な場合には、C2課金情報28を参照して課金処理を行い、C2コンテンツ復号部1217に復号指示を与える。C2コンテンツ復号制御部1216によりなされる課金処理は、C1コンテンツ復号制御部1216によりなされる課金処理と同様であり、通信回線を介して、ユーザが予め契約している銀行等の口座から、音楽コンテンツの供給会社等に、購入料金を送金するような旨の指示情報を送信することである。前記指示情報は、メモ리카ードライタ1200のPCインタフェース1204を介してパーソナルコンピュータ1100の制御部1120により通信回線1001に転送される。なお、C2コンテンツ復号制御部1216は、カウンタ値を記憶し、C2コンテンツの復号毎にカウンタ値を1増加して、このカウンタ値と購入料金の積を求めることにより、例えば1日における購入料金合計の送金指示を夜間に通信回線を通じて行うこともできるものである。

【0033】C2コンテンツ復号部1217は、管理情報復号部1215により復号された管理情報20中のC2アドレス26を参照して暗号化C2コンテンツ140の位置を特定し、管理情報20中のC2鍵25を用いて、暗号化C2コンテンツ140を復号し、オーディオデータであるC2コンテンツをオーディオデータ暗号化部1223に伝える。なお、復号アルゴリズムは、図4に示す暗号化2に対応するブロック暗号方式のアルゴリズムである。

【0034】また、認証部1224は、メモ리카ード1300に含まれる認証部1301との間で、相互に認証をする機能を司る。認証部1301は、メモ리카ードへデータの記録を行う装置側の正当性を認証するもので、認証部1224は認証部1301から認証情報を受信して、この認証情報に基づいて前記メモ리카ードの正当性

11

を判断するものである。なお、認証の方法としては、例えば、メモリカードライタ1200の認証部1224が乱数をメモリカード1300の認証部1301に送り、認証部1301がこの乱数を秘密の暗号化アルゴリズムにより暗号化して返却するのを受けて、暗号化された乱数を認証部1224が復号アルゴリズムにより復号した結果が、もとの乱数と同値であれば、認証部1301が有する暗号化アルゴリズムと、認証部1224が有する復号アルゴリズムが対応するものであるので、認証に成功したと判断する方法が用いられる。この認証方法は、10メモリカードライタ1200と、メモリカード1300とが、秘密の認証鍵と認証方法を共有し、前記認証鍵を用いたチャレンジレスポンス手順により相互に相手を確認する方法でもよい。

【0035】認証が成功した場合、即ち、メモリカードが正当であると判断した場合には、認証部1224は、メモリカードライタ1200のメモリカードID取得部1230及び記録部1240に、それぞれID取得許可、記録許可の指示を与える。ID取得許可を受けると、メモリカードID取得部1230は、メモリカード201300から固有情報であるメモリカードIDを取得し、これをディスク鍵生成部1218に与え、また、記録許可を受けると、記録部1240は、ディスク鍵暗号化部1220、タイトル鍵暗号化部1222及びオーディオデータ暗号化部1223から出力される暗号化されたデータをメモリカード1300に記録する。

【0036】ディスク鍵生成部1218は、メモリカードID取得部1230から与えられたメモリカードIDに関する情報を一部に含むような64ビットのディスク鍵を生成する。ここで、ディスク鍵とは、記録媒体であるメモリカード全体にわたって共通な鍵データを意味する。ディスク鍵暗号化部1220は、ディスク鍵生成部1218により生成されたディスク鍵を、予め記憶している複数のマスター鍵のうちの1つを用いて暗号化し、同じディスク鍵を、続けて別のマスター鍵を用いて暗号化する処理を繰り返し、マスター鍵の数と同じ数の暗号化ディスク鍵を生成してメモリカードライタ1200内の記録部1240に出力する。

【0037】タイトル鍵生成部1221は、適当な64ビットのタイトル鍵を生成してタイトル鍵暗号化部に与える。ここで、タイトル鍵とは、音楽コンテンツ毎に設定できる鍵データを意味する。タイトル鍵暗号化部1222は、タイトル鍵生成部1221により生成されたタイトル鍵を、ディスク鍵生成部1218により生成されたディスク鍵を用いて暗号化して記録部1240に出力する。また、オーディオデータ暗号化部1223は、C2コンテンツ復号部1217により出力されたC2コンテンツを、タイトル鍵生成部1221により生成されたタイトル鍵で暗号化して、記録部1240に出力する。

【0038】ディスク鍵暗号化部1220、タイトル鍵50

12

暗号化部1222及びオーディオデータ暗号化部1223による暗号化アルゴリズムは、ブロック暗号方式のDESアルゴリズムである。なお、記録部1240は、メモリカード1300中のユーザアクセス可能領域にオーディオデータ暗号化部1223から受け取ったオーディオデータを記録し、メモリカード1300中のユーザアクセスが不可能なシステム領域に暗号化されたディスク鍵及びタイトル鍵を記録する。また、メモリカード1300を挿入可能なメモリカード再生機器は、マスター鍵を保持しているものであり、メモリカード1300の認証に成功すれば、暗号化されたディスク鍵とタイトル鍵とを用いて、上述した記録のための暗号化処理の逆処理を行いオーディオデータを復号することにより音楽を再生する機能を有する。＜動作＞以下、上述の構成を備える音楽コンテンツ再生記録システム1000の動作について説明する。

【0039】図6は、音楽コンテンツ再生記録システム1000の動作を示すフローチャートである。同図に示すように、まず、音楽コンテンツ再生記録システム1000の受信部1110は、ユーザ指示に応じて、音楽コンテンツ供給会社のサーバからインターネットを通じて音楽コンテンツを含むカプセルを受信し、カプセル格納部1130に格納する（ステップS301）。

【0040】これにより、カプセル格納部1130にカプセル100が格納された場合、制御部1120は、音楽コンテンツの試聴、購入、又は処理終了のいずれかをユーザに選択させるための、グラフィカルユーザインタフェース画面をディスプレイ1191に表示する。この後、制御部1120は、ユーザが試聴を選択したことを検出すると（ステップS302）、C1コンテンツ処理部1140に、C1コンテンツの再生指示を行う。これを受けてC1コンテンツ処理部1140は、カプセル固有鍵復号部1143によりカプセル固有鍵を復号し、管理情報復号部1145により管理情報を復号する（ステップS303）。

【0041】管理情報復号部1145により管理情報が復号された後、C1コンテンツ復号制御部1146は、C1復号条件情報23を参照して、例えば、現在、C1コンテンツの試聴許容期限内の日時であることや復号回数が所定回数以内であること等によりC1復号条件が満たされている場合には（ステップS304）、課金処理を行い（ステップS305）、C1コンテンツ復号部1147によりC1コンテンツの復号を行い（ステップS306）、再生部1150により、C1コンテンツを再生してスピーカ1193を鳴らせる（ステップS307）。また、C1コンテンツの試聴許容期限の経過後のようにC1復号条件が満たされていない場合には（ステップS304）、ステップS305からステップS307の処理は行わない。

【0042】また、制御部1120は、ユーザが購入を

13

選択したこと、即ちユーザがメモ리카ードへの記録を要求していることを検出すると(ステップS308)、メモ리카ードライタ1200のC2コンテンツ処理部1210に、C2コンテンツの再生指示を行う。これを受けてC2コンテンツ処理部1210は、カプセル固有鍵復号部1213によりカプセル固有鍵を復号し、管理情報復号部1215により管理情報を復号する(ステップS309)。管理情報復号部1215により管理情報が復号された後、C2コンテンツ復号制御部1216は、C2復号条件情報27を参照して、例えば、現在、C210コンテンツの購入許容期限内の日時である等によりC2復号条件が満たされている場合には(ステップS310)、課金処理を行い(ステップS311)、C2コンテンツ復号部1217によりC2コンテンツの復号を行った後(ステップS312)、メモ리카ードへの記録のための暗号化と記録の処理を行う(ステップS313)。また、C2コンテンツの購入許容期限の経過後のようにC2復号条件が満たされていない場合には(ステップS310)、ステップS311からステップS313の処理は行わない。

【0043】また、制御部1120は、ユーザが処理終了を選択したことを検出すると(ステップS314)、試聴又は購入に関する処理はすべて終了するが、処理終了を選択しなければ、ステップS302に戻る。従って、ユーザは、試聴又は購入を何度も選択することができる。図7は、メモ리카ードへのオーディオデータの記録のための暗号化と記録処理を示すフローチャートである。

【0044】同図に示すように、認証部1224は、メモ리카ード1300を認証し(ステップS401)、認証に成功しなければ、暗号化及び記録は行わず、認証に成功した場合には(ステップS402)、以下の処理を行う。まず、メモ리카ードID取得部1230は、メモ리카ード1300からメモ리카ードIDを取得しディスク鍵生成部1218に与える(ステップS403)。ディスク鍵生成部1218は、与えられたメモ리카ードIDに基づいてディスク鍵を生成する(ステップS404)。

【0045】ディスク鍵暗号化部1220は、生成されたディスク鍵を複数のマスター鍵1219それぞれを用いて暗号化し(ステップS405)、暗号化した複数のディスク鍵を記録部1240を介してメモ리카ード1300に記録する(ステップS406)。ディスク鍵の記録後、タイトル鍵生成部1221は、タイトル鍵を生成し、これをディスク鍵を用いて暗号化し(ステップS407)、暗号化されたタイトル鍵を記録部1240を介してメモ리카ード1300に記録する(ステップS408)。続いて、オーディオデータ暗号化部1223は、C2コンテンツ復号部1217により復号されたC2コンテンツをタイトル鍵を用いて暗号化し、記録部1240

14

0を介してメモ리카ード1300に記録する(ステップS409)。

【0046】このように、音楽コンテンツ再生記録システム1000は、ユーザの要求に応じて、音楽コンテンツの再生及びメモ리카ードへの記録を行うことができる。以上、本発明に係る著作物保護システムについて、実施の形態である音楽コンテンツ再生記録システムに基づいて説明したが、本発明はこれらの実施の形態に限られないことは勿論である。即ち、

(1) 本実施の形態では、メモ리카ードにオーディオデータを記録するメモ리카ードライタは、PCカードであることとしたが、これに限定されることはなく、パーソナルコンピュータと接続可能な機器であればよく、例えばUSB(Universal Serial Bus)等により接続される機器であればよい。また、本実施の形態における受信部1110、制御部1120、カプセル格納部1130、C1コンテンツ処理部1140、再生部1150は、パーソナルコンピュータ1100により実現されるものとしたが、パーソナルコンピュータ1100は、メモリ及びCPUを備えプログラム実行制御機能を有する家電機器であればよく、例えば、インターネット接続機能をもつテレビ受信機であってもよい。

【0047】また、本実施の形態では、C2コンテンツ処理部1210は、電流供給用の導線で巻き付けられ全面的に包まれた耐タンパ性を有するLSIパッケージであることとしたが、耐タンパ性を有すれば、導線で巻き付けられているような形態のものに限定されることはない。

(2) 本実施の形態では、メモ리카ードライタ1200内のC2コンテンツ復号部1217が復号したC2コンテンツであるオーディオデータを、メモ리카ードへ記録するために暗号化することとしたが、この他、直接的に再生することとしてもよい。この場合、メモ리카ードライタ1200にスピーカを接続すると、そのスピーカから音楽が流れるようにもできる。

(3) 本実施の形態では、1つのカプセルに1つの暗号化C1コンテンツと1つの暗号化C2コンテンツが含まれていることとしたが、1つのカプセルに暗号化C1コンテンツ又は暗号化C2コンテンツのいずれかのみが含まれていてもよく、また、複数の暗号化C1コンテンツや複数の暗号化C2コンテンツが含まれていてもよく、これらの含まれ方がカプセル毎に異なることとしてもよい。なお、カプセルにC1コンテンツが含まれる場合にのみ管理情報中にはC1コンテンツに関連する課金等の情報が含まれ、カプセルにC2コンテンツが含まれる場合にのみ管理情報中にはC2コンテンツに関連する課金等の情報が含まれるようにすればよい。

(4) 本実施の形態では、C1鍵が64ビット、C2鍵が128ビット等と、鍵データについての長さを示した

15

が、この長さ限定されることはない。K 1 鍵、K 2 鍵、S 1 鍵、S 2 鍵、トランスポート鍵もそれぞれ別個の長さであってもよい。なお、暗号化カプセル固有鍵 1 1 0 は、K 1 鍵で復号できる鍵と K 2 鍵で復号できる鍵とを合成したものとしていてもよく、また、トランスポート鍵の算出のための排他的論理和計算も、全ビットではなく、所定のビットの排他的論理和としてもよい。また、本実施の形態において示した暗号化アルゴリズムも、DES アルゴリズム等に限定されることはない。また、C 1 コンテンツ復号部における復号アルゴリズム及び C 2 コンテンツ復号部における復号アルゴリズムは、通信回線を介してダウンロードすることができるように構成していてもよい。また、復号アルゴリズムをダウンロードする際には、署名情報を確認してそれが正当なものである場合にしか復号アルゴリズムを取り込まないこととしてもよい。なお、この場合、C 2 コンテンツについての復号アルゴリズムは、メモ리카ードライタ 1 2 0 0 中の ROM 1 2 0 2 に含まれる転送用のプログラムを CPU 1 2 0 1 が実行することにより、パーソナルコンピュータ 1 1 0 0 から PC インタフェース 1 2 0 4 を 20 介して C 2 コンテンツ処理部 1 2 1 0 に書き込まれることになる。また、ディスク鍵暗号化部 1 2 2 0、タイトル鍵暗号化部 1 2 2 2、及びオーディオデータ暗号化部 1 2 2 3 における暗号アルゴリズムについても、上述の復号アルゴリズムと同様な方法で、ダウンロードや、署名確認等を行える構成としてもよい。

【0048】ここで、署名情報の確認は、例えば、著作権保護のための中立的な機関により、復号アルゴリズムと署名情報とが送信されるとすると、署名情報は、秘密鍵により暗号化されているものであるため、ROM 1 2 30 0 2 にその秘密鍵に対応する公開鍵を予め記憶しておく、上述の転送用のプログラムの実行によって、その公開鍵を用いて署名情報を復号することにより確認を行うこととすればよい。

【0049】また、本実施の形態では C 1 鍵及び C 2 鍵は、管理情報中に含まれることとしたが、これに限定されることはなく、C 1 鍵は C 1 コンテンツ復号部に予め記憶されている鍵データであることとしてもよく、C 2 鍵は C 2 コンテンツ復号部に予め記憶されている鍵データであることとしてもよい。

(5) 本実施の形態では、カプセルは通信回線を通じて送られるものとしたが、これに限定されることはなく、光ディスク等の記録媒体に格納されるものであってもよい。この場合、受信部 1 1 1 0 が、カプセルを記録媒体から読み出してカプセル格納部 1 1 3 0 に格納するようになるものであればよい。

(6) 本実施の形態では、タイトル鍵生成部 1 2 2 1 は、適当にタイトル鍵を生成することとしたが、これに限定されることはなく、タイトル鍵生成部 1 2 2 1 は、例えば、C 2 コンテンツ復号部 1 2 1 7 の出力する C 2 50

16

コンテンツを参照して、曲名等のデータに基づいてタイトル鍵を生成するものであってもよく、また、管理情報復号部 1 2 1 5 により復号された管理情報中の C 2 鍵を参照し、これに基づいてタイトル鍵を生成するものであってもよい。また、さらに、タイトル鍵生成部 1 2 2 1 は、メモ리카ードライタ 1 2 0 0 に固有な値に基づいてタイトル鍵を生成するものであってもよい。

(7) 本実施の形態では、ディスク鍵生成部 1 2 1 8 は、メモ리카ード ID に基づいてディスク鍵を生成することとしたが、メモ리카ード ID と無関係にディスク鍵を生成するものとしてもよい。また、メモ리카ード中にマスター鍵により暗号化された媒体に固有な固有ディスク鍵が記録されているものとしてもよく、これに対応して、ディスク鍵生成部 1 2 1 8 は、この固有ディスク鍵を、マスター鍵を用いて復号することにより、ディスク鍵を生成することとしてもよく、この場合には、ディスク鍵暗号化部 1 2 2 0 は不要となり、従って記録部 1 2 4 0 により暗号化したタイトル鍵及び暗号化したオーディオデータのみがメモ리카ードに書き込まれるようにすればよい。

(8) 本実施の形態では、オーディオデータ暗号化部 1 2 2 3 は、C 2 コンテンツであるオーディオデータを暗号化するものとしたが、C 2 コンテンツの一部を暗号化して出力することとしてもよい。

(9) 本実施の形態では、マスター鍵は C 2 コンテンツ処理部内に予め複数記憶されていることとしたが、これに限定されることはなく、単数であってもよい。また、C 2 コンテンツ処理部は、通信回線及びパーソナルコンピュータを介して外部ネットワークからマスター鍵をダウンロードして取り込み記憶することとしてもよく、特定のマスター鍵を削除する機能を有するものであってもよい。また、マスター鍵をダウンロードする際には、署名情報を確認してそれが正当である場合にのみマスター鍵を取り込むこととしてもよい。なお、この場合、マスター鍵は、メモ리카ードライタ 1 2 0 0 中の ROM 1 2 0 2 に含まれる転送用のプログラムを CPU 1 2 0 1 が実行することにより、パーソナルコンピュータ 1 1 0 0 から PC インタフェース 1 2 0 4 を介して C 2 コンテンツ処理部 1 2 1 0 に書き込まれることになる。こ
40 で、マスター鍵についての署名情報の確認も、上述の復号アルゴリズム等についての署名情報の確認と同様な方法で行えばよい。同様に、特定のマスター鍵の削除指示を外部ネットワークから受け付けた場合にも、署名情報を確認してそれが正当である場合にのみ特定のマスター鍵を削除することとしてもよい。

(10) 本実施の形態では、メモ리카ードの認証を行い(ステップ S 4 0 1)、認証に失敗した場合には暗号化及び記録を行わないこととしたが(ステップ S 4 0 2 等)、認証に失敗した場合に最終的にメモ리카ードへの記録がなされなければよいのであって、例えば、認証に

17

失敗するか否かにかかわらず暗号化は行い、認証に失敗したならば暗号化の結果生じるデータのC2コンテンツ処理部1210からの出力を抑止するようにしてもよい。

(11) 本実施の形態で示したメモ리카ードへ暗号化したデータを記録するため手順は(ステップS406、S408、S409)、この順に限定されることはなく、いかなる順序で実行されるものであってもよい。また、同じメモ리카ードに複数のコンテンツのデータを記録することもでき、この場合、タイトル鍵生成部1221 10は、コンテンツの数だけタイトル鍵を生成し、タイトル鍵暗号化部1222も前記コンテンツの数だけの暗号化されたタイトル鍵を出力し、オーディオデータ暗号化部1223も前記コンテンツの数だけの暗号化されたデータを出力する。

(12) 本実施の形態では、著作権保護センタによりカプセルが生成されることとしたが、これに限定されることはなく、コンテンツ提供者やプロバイダ等が生成することとしてもよい。また、この場合に鍵データの安全性を高めるため、コンテンツ提供者やプロバイダ等が公開20鍵を使ってカプセル固有鍵を暗号化し、再生装置側が、当該公開鍵に対応する秘密鍵を用いて復号することとしてもよい。

(13) 本実施の形態では、課金処理として、送金の指示情報等が送信されることとしたが、これに限定されることはなく、課金情報に復号した回数等を含ませ、この課金情報を課金機関向けに暗号化して送信することとしてもよい。また、この際、課金情報をコンテンツとみなし、カプセルと同一のフォーマットで暗号化して送信することとしてもよい。このためには、C1コンテンツ処理部1140及びC2コンテンツ処理部1210にカプセルを生成するための暗号化部を設ければよい。当該暗号化部における暗号化は、図4、図5に示したカプセル生成の手順に従って行うものとすればよい。

【0050】なお、記録部1240が、メモ리카ード等の記録媒体にコンテンツを記録する際に、管理情報に含まれる復号条件情報や課金情報をも記録することとしてもよい。この場合にも、復号条件情報や課金情報は暗号化等により安全な状態で記録することとしてもよい。これにより、記録媒体に記録後もコンテンツの再生の実行40を制御したり再生実行に対して課金したりすることを可能にできる。

【0051】

【発明の効果】以上の説明から明らかなように、本発明に係る著作物保護システムは、外部から入力されたデジタル著作物である暗号化されたコンテンツを復号し、記録用に再暗号化して出力する著作物保護システムであって、入力されたコンテンツを第1の暗号方式で復号する復号手段と、前記復号手段により復号されたコンテンツの全部又は一部を第2の暗号方式で暗号化して出力する50

18

暗号化手段とを備え、前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータの通信路が単一の耐タンパ性のあるパッケージに封入され、外部との入出力のための端子が前記パッケージの外部に表出しており、前記復号手段は、前記端子を通じて入力を受け付け、前記暗号化手段は、前記端子を通じて出力することを特徴とする。

【0052】これにより、暗号化されたコンテンツを一度復号して再度暗号化する過程において、復号されたコンテンツが不正に覗き見されないようになる。また、前記復号手段、前記暗号化手段、及び前記復号手段から前記暗号化手段へのデータ通信路は、1チップの半導体集積回路から構成されていることとすることもできる。

【0053】これにより、復号から再暗号化までの過程が1つのチップ内でなされるため、復号された無防備なコンテンツが電氣的、物理的に覗き見することができなくなる。また、前記復号手段あるいは前記暗号化手段は、鍵データを記憶しており、復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムを、前記端子を通じて外部ネットワークよりダウンロードし、前記コンテンツを前記鍵データを用いて前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記鍵データを用いて前記暗号アルゴリズムにより暗号化することとすることもできる。

【0054】これにより、コンテンツについての暗号化アルゴリズムを随時変更し得るので、暗号の安全性が向上する。また、前記復号手段はさらに、前記端子を通じてコンテンツの復号に関する暗号化された制御情報を取得すると共に取得した制御情報を復号する制御情報復号部と、前記復号部により復号された制御情報に基づいて前記コンテンツの復号を行うコンテンツ復号部とを有することとすることもできる。

【0055】これにより、コンテンツの復号に関する制御情報、例えば復号条件や課金情報等が、暗号化されているため、コンテンツの復号に関する制御情報の覗き見や改ざんを防止できる。また、前記暗号化手段は、マスター鍵を記憶するマスター鍵記憶部と、ディスク鍵を生成するディスク鍵生成部と、前記マスター鍵を用いて、前記ディスク鍵生成部により生成された前記ディスク鍵を暗号化するディスク鍵暗号化部と、タイトル鍵を生成するタイトル鍵生成部と、前記ディスク鍵を用いて、前記タイトル鍵生成部により生成された前記タイトル鍵を暗号化するタイトル鍵暗号化部と、前記タイトル鍵を用いて、前記復号手段により復号されたコンテンツの一部又は全部のデータを暗号化するデータ暗号化部と、前記ディスク鍵暗号化部により暗号化されたディスク鍵と、前記タイトル鍵暗号化部により暗号化されたタイトル鍵と、前記データ暗号化部により暗号化されたデータとを前記端子を通じて出力する出力部とを有することとすることもできる。

19

【0056】これにより、ディスク鍵、タイトル鍵、データと3層化して暗号化し、マスター鍵を有する装置によらなければデータの復号ができないので記録媒体に記録されたデータの安全性は高まり、一般ユーザによる不正コピーが防止できる。また、ディスク鍵及びタイトル鍵を、記録媒体中のユーザがアクセス不可能な領域に書き込むことによりさらに安全性を高められる可能性を持つ。なお、記録媒体がDVDである場合には、DVD再生機器に対応できる。

【0057】また、前記マスター鍵記憶部は、複数のマ10スター鍵を記憶し、前記ディスク鍵暗号化部は、複数の前記マスター鍵それぞれを用いて、前記ディスク鍵を暗号化することにより、複数の暗号化されたディスク鍵を生成することとすることもできる。これにより、メーカー毎に異なるマスター鍵を用いることとすれば、複数のメーカーの記録媒体再生装置により、記録媒体に暗号化された記録されたデータの復号が可能となる。また、単一のマスター鍵ではなく複数のマスター鍵を用いるため、記録媒体再生装置への攻撃に対する安全性が高まる。

【0058】また、前記暗号化手段はさらに、前記マス20ター鍵を外部ネットワークよりダウンロードして前記マスター鍵記憶部に追加する、あるいは、特定マスター鍵を無効化するマスター鍵制御部を有することとすることもできる。これにより、マスター鍵を追加することができるため、新たな記録媒体再生装置が生産された場合にも対応できる。

【0059】また、前記暗号化手段により暗号化の結果として得るデータは、記録媒体に記録されるべきものであり、前記記録媒体には、予め媒体に固有な固有情報が記録されており、前記ディスク鍵生成部は、前記記録媒30体中の前記固有情報に基づいて前記ディスク鍵を生成することとすることもできる。

【0060】これにより、記録媒体毎に異なる暗号化が行えるので暗号の安全性が高まり、また、記録媒体からデータを再生する装置側において、ディスク鍵と、記録媒体中の固有情報とを参照することにより記録が正当に行われたものか否かを調べることができ、正当なものである場合にのみ再生を行うようにすることもできる。また、前記タイトル鍵生成部は、前記復号手段により復号されたコンテンツの一部の情報、又は前記暗号化手段に40固有な情報に基づき、前記タイトル鍵を生成することとすることもできる。

【0061】これにより、コンテンツ毎に異なる暗号化が行えるので暗号の安全性が高まり、また、不正コピーがなされた場合に不正な機器の特定に役立つことが期待できる。また、前記記録媒体は、記録装置認証部を備え、前記出力部は、前記記録媒体の前記記録装置認証部から受信する認証情報に基づいて前記記録媒体の正当性を判定し、正当である場合にのみ、前記出力を行うこととすることもできる。

20

【0062】これにより、内容の覗き見が容易な不正な記録媒体への記録を防止することができる。また、前記復号手段は、前記コンテンツの復号に際し、当該復号に対する課金処理を行うこととすることもできる。これにより、コンテンツの復号に対して料金を課することが可能となり、コンテンツの販売が容易となる。

【0063】また、前記復号手段あるいは前記暗号化手段は、外部ネットワークよりダウンロードした復号アルゴリズムを記述したプログラムあるいは暗号アルゴリズムを記述したプログラムについて署名情報を確認して、正当であった場合にのみ、以後、前記コンテンツを前記復号アルゴリズムにより復号する、あるいは、復号したコンテンツを前記暗号アルゴリズムにより暗号化することとすることもできる。

【0064】これにより、出所の正当な復号アルゴリズムあるいは正当な暗号アルゴリズムのみを取得することができるので、不正なアルゴリズムの置換を防止できる。また、前記マスター鍵制御部は、外部ネットワークよりダウンロードした前記マスター鍵について署名情報を確認して、正当であった場合にのみ、前記マスター鍵を前記マスター鍵記憶部に格納する、あるいは、無効化制御について、署名情報を確認して、正当であった場合にのみ、前記特定マスター鍵の無効化を行うこととすることもできる。

【0065】これにより、出所の正当なマスター鍵のみを取得することができるので、不正利用を防止できる。また、前記パッケージは、記録媒体に前記コンテンツを記録する記録装置に内蔵され、前記暗号化手段は、前記記録媒体に前記コンテンツの全部又は一部を記録するための所定の規格化された暗号化方式に従った暗号化を行うものであり、前記復号手段に入力される前記コンテンツに施されている暗号化は、前記コンテンツの配送元と、前記記録装置との間における特有の暗号化方式により、前記コンテンツを安全に配送するためになされたものであることとすることもできる。

【0066】これにより、記録媒体への記録装置に対しての配送のために暗号化されて送られるコンテンツを、記録媒体への記録用の規格化された暗号化に変えて記録することができ、この暗号の変換の過程で生ずる生のコンテンツを覗き見されることがないので、記録装置への配送から記録媒体の記録までの一連の過程における安全性が確保される。

【図面の簡単な説明】

【図1】本発明に係る著作物保護システムの実施の形態である音楽コンテンツ再生記録システム1000の外観図である。

【図2】音楽コンテンツ再生記録システム1000の機能ブロック図である。

【図3】メモ리카ードライタ1200のハードウェア構造を示す図である。

【図4】暗号化C1コンテンツ130及び暗号化C2コンテンツ140の生成過程を示すデータフロー図である。

【図5】暗号化カプセル固有鍵110及び暗号化管理情報120の生成過程を示すデータフロー図である。

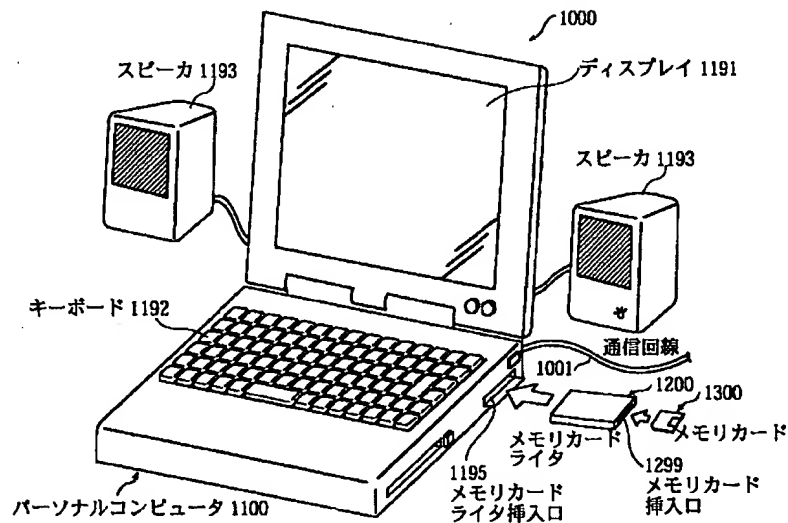
【図6】音楽コンテンツ再生記録システム1000の動作を示すフローチャートである。

【図7】メモリカードへのオーディオデータの記録のための暗号化と記録処理を示すフローチャートである。

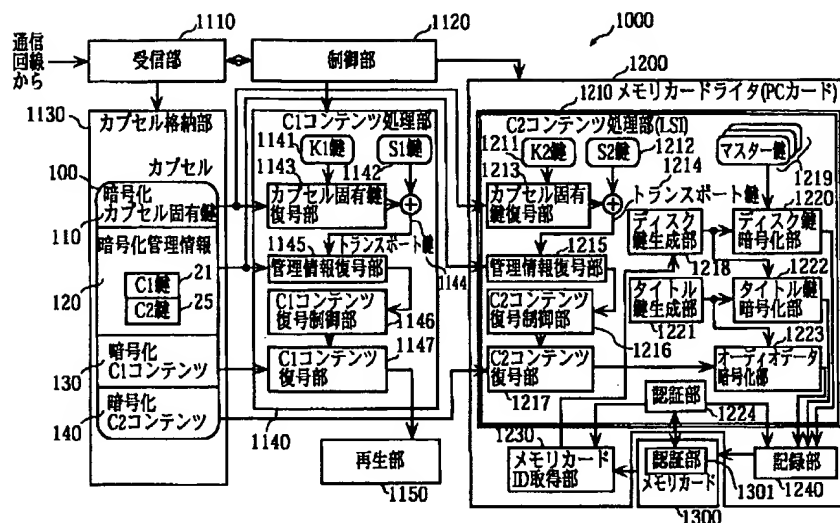
【符号の説明】

1000	音楽コンテンツ再生記録システム	1193	スピーカ
1001	通信回線	1195	メモリカードライタ挿入口
1100	パーソナルコンピュータ	1200	メモリカードライタ
1110	受信部	1201	CPU
1120	制御部	1202	ROM
1130	カプセル格納部	1203	RAM
1140	C1コンテンツ処理部	1204	PCインタフェース
1143	カプセル固有鍵復号部	1205	メモリカードインタフェース
1145	管理情報復号部	1210	C2コンテンツ処理部
1146	C1コンテンツ復号制御部	1213	カプセル固有鍵復号部
1147	C1コンテンツ復号部	1215	管理情報復号部
1150	再生部	1216	C2コンテンツ復号制御部
1191	ディスプレイ	1217	C2コンテンツ復号部
1192	キーボード	1218	ディスク鍵生成部
		1220	ディスク鍵暗号化部
		1221	タイトル鍵生成部
		1222	タイトル鍵暗号化部
		1223	オーディオデータ暗号化部
		1224	認証部
		1230	メモリカードID取得部
		1240	記録部
		1299	メモリカード挿入口
		1300	メモリカード
		1301	認証部

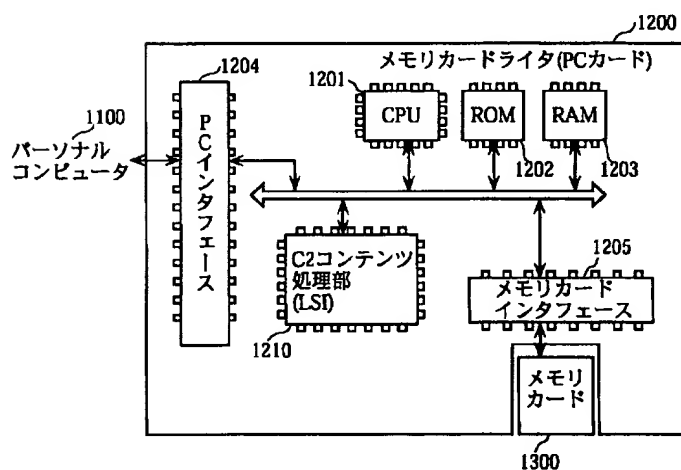
【図1】



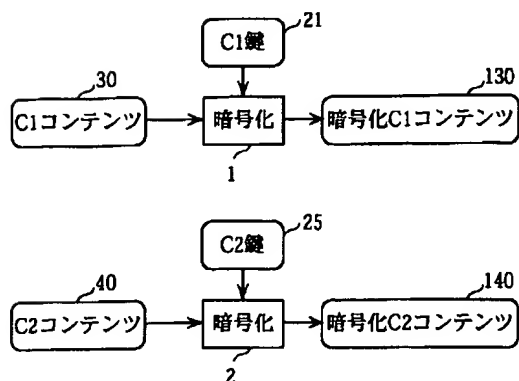
【图 2】



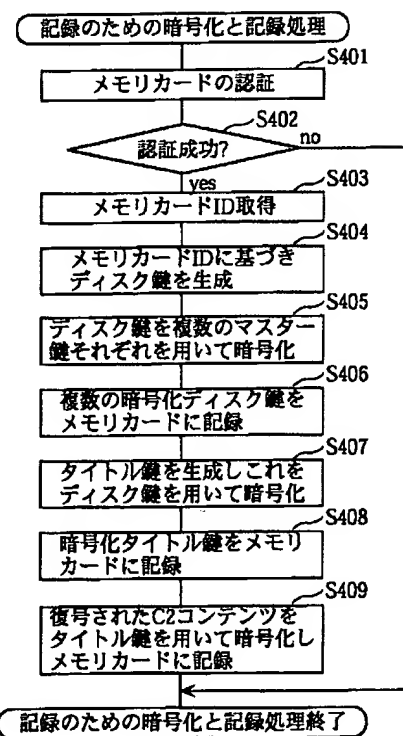
【图 3】



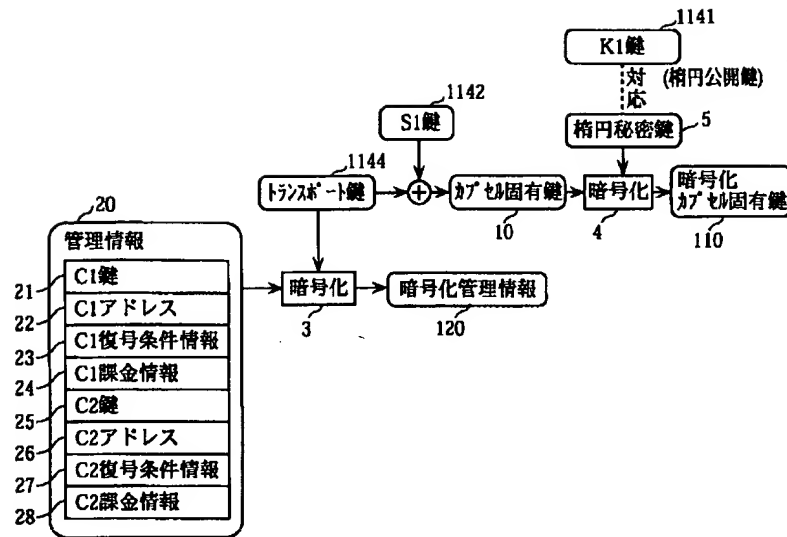
【図 4】



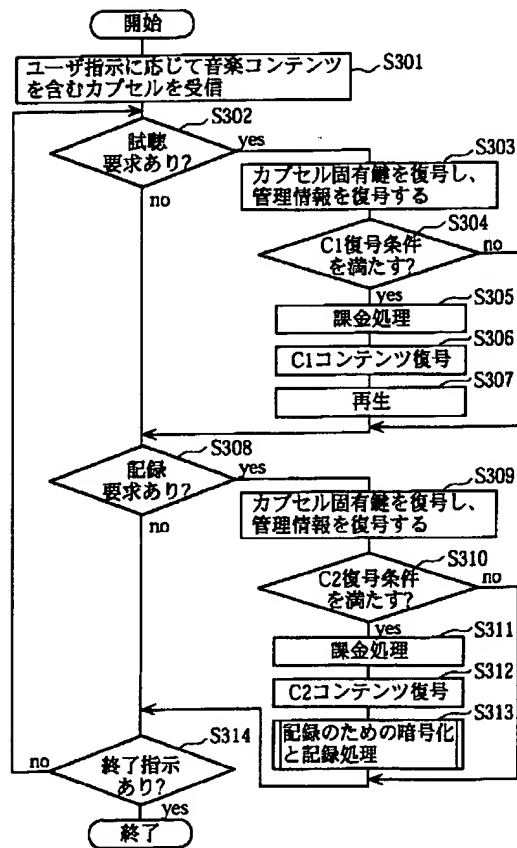
【図 7】



【図5】



【図6】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

ターム(参考)

H O 4 L 9/10

H O 4 L 9/00

6 2 1 A

F ターム(参考) 5B017 AA06 BA05 BA07 BB03 BB07
CA11 CA14 CA16
5D044 AB05 CC04 GK17 HL01 HL11
5J104 AA07 AA46 JA21 KA02 KA05
NA05 NA36 PA05 PA07 PA10

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.